Have you done enough to protect your trade secrets?

August 1, 2006

By Ralph Kroman

Recent cases in the news have demonstrated that a company may go to great lengths to acquire the confidential information of a competitor. An unscrupulous company will use sophisticated technology to acquire confidential information, and a business should not underestimate its competitors.

Although appropriate means will reduce the likelihood of hacking and other electronic intrusions, competitors often acquire confidential information such as customer lists through employees. If an employee leaves a business and discloses confidential information to a competitor, it can be very difficult to prove in court that confidential information was disclosed. When dealing with confidential information, the age-old adage applies: “an ounce of prevention is worth a pound of cure”.

Employees who have access to confidential information should sign agreements which contain appropriate confidentiality clauses. The courts will enforce non-solicitation and noncompetition clauses under appropriate circumstances. The agreement should be drafted to contain provisions which are appropriate so that a court will not frown upon them. Many companies have signed confidentiality agreements in their files but often they overlook the importance of employee entrance and exit interviews.

During an entrance interview, each new employee should be reminded of his or her obligations regarding the company’s confidential information. The information which the company considers confidential must be clearly identified to the employee. A company policy regarding confidential information should be reviewed with the employee and a receipt obtained from the employee.

A wise employer also tells the employee during the initial interview that the employee must not disclose confidential information of former employers. The agreement which is signed by the employee should contain a representation and warranty to this effect. Recent legal cases have shown that, if an employer turns a blind eye to the disclosure of confidential information of a third party to it, the directors and officers of the employer may be held personally liable.

If an employee signs a confidentiality agreement after employment has commenced, it must be structured properly or else the agreement will be unenforceable. The courts like to see that the employee gave consideration for the agreement and the lack of consideration may render the agreement unenforceable.

It is imperative that employees who depart employment are given proper exit interviews where their legal obligations regarding confidential information are explained. Employees will likely be more reluctant todisclose confidential information to a new employer if they know that the former employer is serious about protecting its interests. It should be confirmed by the employee that no copies of confidential information remains in the hands of the employee, and the employee’s passwords should be de-activated (in the Air Canada/ WestJet case, the passwords of a former employee were used by a competitor).

If the former employee will be employed with a competitor under suspicious circumstances, an appropriate letter should be sent to the new employer. This letter does not need to be adversarial but is intended to put the new employer “on notice” that the new

employer must not use confidential information disclosed to it.

Relationships with independent contractors and consultants can be soft spots for companies with confidential information. The general rule is that, unless there is an agreement to the contrary, independent contractors own all of the deliverables. If a dispute arises with an independent contractor, companies often find themselves in precarious positions regarding deliverables unless an agreement states that the company owns the deliverables. This issue has resulted in a great deal of litigation which could be avoided by appropriate language in an independent contractor agreement.

The more effort that a company makes to treat information as confidential, the greater the protection that courts will give to it. Additional steps which may be taken include:

- Preparation of a list which inventories all confidential information which is coupled with accessibility policies
- Numbering hard copies of documents containing confidential information
- Maintenance of a logbook regarding copies of confidential information which are disclosed to employees

One of the best ways to protect confidential information is with a “confidential stamp” which is placed on each electronic or hard copy of a document. It is preferable that this stamp appears on each page. Many companies simply stamp “confidential” but the stamp is more effective if it includes the name of the owner of the confidential information, states that copying is not permitted without the express or consent of the owner, and confirms that the document and all copies of the document are the sole property of the owner.

It is common practice today for businesses to exchange confidential information in order to further the negotiation of a business deal. It is standard practice that “standard form” non-disclosure or confidentiality agreements are signed. However, the fine print should be reviewed. Some agreements require that confidential information which is disclosed orally, must be confirmed in writing within a certain number of days. If it is not feasible to comply with this obligation, the agreement should be amended.

In any event, when a company discloses confidential information, it should be marked with or contain a “confidential stamp”, and the disclosing party should maintain a file which contains proof of the delivery of the confidential information including an exact copy of all information disclosed, the date of the delivery and the identity of the recipient. The cover letter should list the enclosures and highlight the confidential nature of the information.

On the whole, it is important for a company to recognize that protecting confidential information is not simply a matter of adopting a “cookie cutter” approach. A protection plan should be customized to reflect the type of information and the commercial realities of the business. Unfortunately, many companies do not focus upon a plan until it is too late.

For more information or inquiries:

Ralph Kroman

Toronto
416.947.5026

Email:
rkroman@weirfoulds.com

Ralph Kroman brings broad experience and high-level expertise to his business law practice with an emphasis upon contract negotiations, intellectual property, information technology and commercial transactions.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035

© 2025 WeirFoulds LLP